CONVERTER MAGAZINE
Volume 2021, No. 4

Key Technologies of IoT Service Security and Privacy Protection

Dongxian Yu[1,*], Jiatao Kang[2], Junlei Dong[1]

[1]College of Information and Engineering, Henan Polytechnic, Zhengzhou, Henan, China

[2] Department of Architectural Engineering, Henan College of Transportation, Zhengzhou, Henan, China

**Corresponding author.*

Abstract

The Internet of Things in the industrial industry has attracted widespread attention from the government, academia, and industry due to its huge application prospects. The core ideas of the Internet of things are perception, control, transmission and intelligence. Through technical means to achieve the coordination between things, people and things, and people, so as to form a larger complex network system on the basis of sensor network, Internet and mobile communication network. The data Shared by Internet of things information is closely related to personal life behaviors, and the information has a greater perceived correlation with each other. This kind of sensibility and sensitivity put forward higher requirements for the security and privacy protection of Internet of things information sharing. However, due to the characteristics of network structure, terminal equipment, communication mode and application scenario, some security and privacy issues unique to the Internet of things cannot be solved directly through existing Internet security technologies. It is necessary to conduct in-depth research on the key technologies of Internet of things security and privacy protection. This article briefly describes the Internet of things security and privacy issues, then, it gives the research and application status of Internet of things security and privacy protection at home and abroad, then lists the key technical problems in Internet of things security and privacy protection. And for communication between large scale collaborative services. Based on publish/subscribe paradigm, this paper constructs collaborative communication facilities of Internet of things services suitable for large-scale distribution, and an access control architecture for managing service synergy interactions, achieve confidentiality of data exchange between services and privacy protection of service policies.

Keywords: *Industrial industry, internet of things, service security, privacy protection, collaborative interaction*

I. Introduction

Facing the various physical targets in the real world, intelligent terminal devices help the Internet of Things system to realize the analysis, collection, timely or delayed analysis and processing of information data[1-3]. Through the connection of the wired/wireless network system, the Internet of Things system finally completes “perception and communication” with various physical targets in the real world. In a broad sense, the Internet of Things system can be considered as a type of "Internet" for information data recognition and communication between a wide area network/local area network, a person and a target that needs to be recognized[4]. At present, there are many immature places in the technology of the Internet of Things system, and there is a widespread situation in which data information is not encrypted and transmitted directly in the Internet of Things system. Various types of sensors and network systems are at risk of being compromised by potential intruders[5-8]. Therefore, it is of great practical significance to analyze and research the Internet of Things system in terms of system security and promote the gradual improvement of the Internet of Things system. In the past ten years, with the rapid development of information network technology and sensor technology, emerging fields such as artificial intelligence,cloud computing, Internet of Things, big data,etc. have also developed rapidly. The progress of Internet of Things technology and the expansion of application fields, the Internet of Things system the production cost of related equipment and equipment has dropped rapidly, and many information, automation and intelligent IoT technologies have been gradually applied to various intelligent industrial control systems. The Internet of Things system has brought huge social and economic benefits to customers[9]. At the same time, the security issues of IoT systems in intelligent industrial control systems have surfaced. At this stage, with the development of industrial Internet of Things, IT and OT are gradually integrated [10-14]. As an important part of the "Industry 4.0" project, the IoT system, the production equipment, the industrial software system and the production control system are interconnected through the Industrial Internet of Things. This situation has made the IoT system security threat difficult to detect and the IoT system security After the risk issue, it is more difficult to conduct investigations and repairs [15].

The Internet is the foundation of IoT construction, so the security threat of the Internet of Things includes two aspects. First of all, the security problems encountered in the Internet will appear in the Internet of Things; secondly, the IoT system itself and related applications are also vulnerable. At present, the status quo of China's network security is not optimistic[16-18]. First, in the public Internet environment, the traits of hacker attacks are becoming more and more obvious. The criminals aim at communication networks, information systems, and user information and property. They use hacker technology to launch cyber attacks to gain illegal interests, and gradually form a tight organization and division of labor. Clear Internet underground industry[19-21]. For the security of the Internet of Things system itself, it is mainly reflected in the perception layer of the Internet of Things. In the overall architecture of the Internet of Things, the perception layer is at the bottom and the most basic level. Information security at this level is the most vulnerable. The sensing layer mainly uses RFID and WSNs in the process of collecting information. The security of the Internet of Things perception layer is essentially a security issue for RFID systems and WSNs systems[22]. When sensors receive information through WSNs, they will need a large number of sensor nodes. These nodes are often exposed to public places, remotely controlled by people or computers, lacking effective protection, and easily interfered with signal interference or even node capture. Furthermore, there are many security vulnerabilities in the routing protocols of WSNs, and criminals can inject malicious routing information into WSNs to make the network paralyzed. With the rapid application and application of RFID technology, its data security problem has even exceeded the security boundary of the original computer information system in some areas, and has become a widespread concern[23]. The main reason is: the card computing power is weak; the vulnerability of the wireless network causes the transmitted information to be exposed to the public; the privacy and security of the business application makes the security and privacy of the transmitted information an important factor restricting the further development of the Internet of Things.

In view of the characteristics of IoT services and the above security and privacy challenges, this paper has conducted in-depth research on the key issues of security and privacy protection technologies for services in the IoT environment. Researching highly scalable data access control, services and user privacy protection mechanisms provides theoretical guidance and practical value for building secure IoT services.

II. Proposed Method

2.1 Privacy protection

Privacy is a concept formed by human society in the context of the concept of private ownership in the civilized era. Privacy is defined differently for different domains and objects. The first privacy is defined as the right to maintain personal solitude, and later privacy is defined as the right of individuals to decide and control the sharing and use of their information by others. There is no clear definition of a more general and broad concept of privacy. This article believes that for personal or collective security and interests, the information that is closely related to itself is hidden to prevent outsiders from knowing that such hidden information is "privacy." Privacy information is information that individuals, groups, and other entities are reluctant to be aware of by the outside world. This information is related to the security and interests of the entity, including sensitive data and characteristics characterized by the data, such as the patient's condition, personal compensation, and company financial information. Wait. The act taken to achieve covert privacy information is called "confidentiality of privacy protection", that is, "privacy protection."

In order to provide users with ubiquitous personalized services, the Internet of Things needs to use the automatic sensing function to use the user's personal information without the user's awareness or interference. For example, in the intelligent medical care system, it is necessary to collect physiological physiological data (heart rate, body temperature, blood pressure, etc.) of the user in real time. In the IoT environment, the use of personal information covers the entire life cycle of users' personal data, including its perception, storage, transmission and application. User privacy issues mainly occur in the sensing and application phases of these four processes. Data perception has the characteristics of invisible and wide coverage, and belongs to system behavior. Because perceived personal information is private to users, users have privacy protection requirements for this process. In addition, service-oriented application processing the essence is that the personal information is shared by other entities interacting with the system. For individuals, the information is uncontrollable, and the user also needs privacy protection for this process. In these cases, if the system privacy protection mechanism is missing, the user's private information will be potentially threatened, which raises the privacy protection of the Internet of Things. As a special concept, privacy protection has the timeliness and mandatory characteristics of time and space in the historical process of each entity. Although it is for unauthorised persons, privacy protection has its special significance compared with the privacy of information security in general. Privacy can be considered as the privacy of certain information, and unlike general information privacy, in many cases, privacy and external needs must be balanced. For example, when a doctor provides a diagnosis service to a patient, some patients may be ashamed to disclose their personal information, but have to provide their doctor with their own historical medical records. The source of balance between external demand and privacy protection is often due to political or other social coercive factors. In addition, privacy protection has a broader, relatively independent system and variability for different spaces and times. Therefore, the goal of privacy protection technology is not to completely hide private information, but to meet the certain information needs of the outside world while leaking as little as possible, that is, to balance external needs and privacy protection. Privacy protection technology refers to the general term for all technologies that can be used to protect privacy. From the perspective of protecting privacy information, access control and physical security,digital identity authentication are the most widely used privacy protection technologies. Individuals use information hiding technology, encryption and decryption technology and anonymous technology to protect the privacy of personal information.

2.2 Strategy Synthesis Research for Secure Data Sharing

In order to provide better services to users, different organizations need to cooperate with each other. The main goal of this collaboration is data sharing. Data shared in a service collaborative environment is generally sensitive, such as medical data for patients in a medical information system. Therefore, providing security guarantees for sharing data is an urgent problem to be solved. Access control is an important part of data security and privacy, and its aim is to prevent unauthorized users from illegally accessing protected data. However, access control for shared data can be challenging due to the involvement of different organizations.To meet this challenge, a common global strategy needs to be developed for each participating organization, which can be accepted by all participating organizations. The development of a global strategy usually requires a coordinated or negotiated approach between the organizations. In the case of service composition, policy generation for composite services requires a policy that integrates each component service together.Therefore, the key to determine the access control policy of shared data is to merge the local policies of different participating organizations into a global policy. In general, there are two layers of strategy for shared data—the layer is a coarse-grained data layer, the organizational layer, files, databases and other information; the other layer is the data layer associated with the data structure. The research in this section focuses on the coarse-grained data layer. In a collaborative environment across organizations, shared data is typically managed and owned by different organizations. To protect data, different organizations often choose different attribute elements and access control constraints to independently formulate policies to manage how the data is used, which can easily lead to misunderstandings between organizations.And the strategies of different organizations are different, even repellent, such as one rule allows some operation on shared data, and another rule does not allow the same operation on shared data. Therefore, how to integrate and standardize policy rules, how to solve different and even repelled rules is a key issue in the strategy combination. To solve the above problem, the first quest is to standardize the access control policy requirements of every participating organization. Strategic languages play an important role in regulating these requirements. A variety of languages have emerged, such as XACML, EPAL, and XACL, which have provided some strategy combination algorithms. But they focus on pre-canonical strategy combination algorithms, for example allowing priority, rejecting priority, and so on. These methods are not sufficient to support complex policy combination semantics based on data sharing. For example, XACML does not include a more rigorous policy combination algorithm, that is, when all policies allow a request, the combined policy also allows the request; as long as any rule rejects a request, the combined policy rejects the request. This article will use this strategy to combine rules to combine strategies.

XACML is one of the most commonly used policy specification languages, and it provides a more flexible way to manage the elements in each strategy. XACML supports attribute based access control policy model, which makes attribute based constraint rule one of the popular access control methods in distributed cooperative environment. Therefore, we mainly consider attribute-based strategy combinations. In addition, XACML specifies multiple policy/rule combination algorithms; Permit-unless-Deny: PD, etc., unless rejected. Each XACML policy contains multiple rules. If an organization combines these rules with different rule combination algorithms, they will get different strategies. For example, organization A uses the P0 combination algorithm to combine their rules. If there is a rule that allows a request, the result of the combination allows the request; and if organization A uses the DO combination algorithm to combine their rules, if there is a rule that rejects a request, the result of the combination rejects the request. Therefore, it is necessary to consider the institution combination algorithm used by different strategies in the strategy combination. In the XACML strategy, conditional constraints are restrictions on attributes. The existence of multiple conditional constraints in a strategy makes the strategy combination process complicated. Algebraic theory can be used to construct a policy framework that describes the behavior of a strategy combination and verifies the validity of the combined results. These algebraic systems can deal with limited constraints, which provides theoretical support for the research work in this paper. Determining a global strategy for sharing data across organizations is a challenging issue. From the perspective of the requester, in order to determine whether the request can access the shared data, it is necessary to determine whether the attributes of the request meet the global policy of the cooperative organization, which requires the combination of the local policies of different organizations into a global policy. The results of the combination are not only consistent with the individual local strategies, but also by the various collaborative organizations. Therefore, it is necessary to choose the appropriate XACML rule combination algorithm in the Innovative strategy. There is currently no automated strategy synthesis tool that automatically combines different local strategies into one global strategy rather than a policy decision. This paper proposes a multi policy composition architecture and develops an automatic policy composition tool using rule reduction method. The tool can automatically generate a global strategy when entering local strategy for different organizations. Based on the criterion specification of XACML, the FIA algebra system is extended to support different types of attributes in the rules by defining a reduction rule. The multi-strategy combination process is mainly divided into three steps. First, the rules are classified according to the condition constraints in the rules. Secondly, the conditional constraints with the same attributes are reduced to one class. Finally, the conditional attribute values In the same rules are compared, and the class is compared. The rule is reduced to the rule in the global strategies.

2.3 Service Access Control Based on Publish / Subscribe System

The smart grid will be the foundation of the next-generation grid system. Its goal is to enable two-way real-time interaction between data providers and data consumers through the integration of the power grid and communication networks. Integration requires communication systems that are loosely coupled, configurable, and open. In the smart grid, data is distributed in real time and should be secured. The existing intelligent grid communication system mainly adopts the request/response interaction model. The data access is directly controlled by the data provider, and the direct control interaction model can not extend the complex interactive services supporting the smart grid. However, the publish/subscribe model has loosely coupled features between data providers and data consumers, allowing the publish/subscribe system to allow smart grid services to perform indirect, anonymous, and multicast interactions. The publish/subscribe system therefore supports scalable, flexible interaction between smart grid services. The GridStat project uses a publish/subscribe model to build a collaborative smart grid service data interaction architecture. The communication architecture in Figure 1 can provide QoS-differentiated real-time data, such as data collected by the base station phasor data concentrator and passed the substation phasor test.

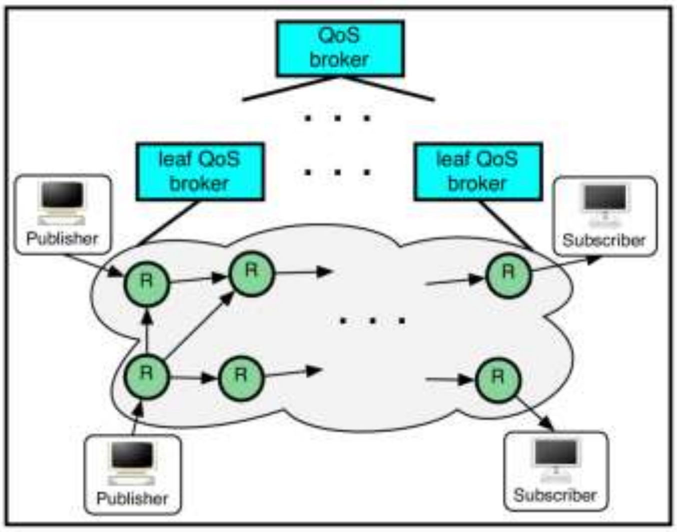

Figure 1. Grid Stat communication facility

In a publish/subscribe-based service data owners, data consumers interact indirectly, interaction model and multicast by notifying the proxy network. The data consumer expresses its interest by subscribing, without knowing who posted the data, and the data producer publishes the data without knowing who used its data. In the publish subscription mode, the interaction of data is anonymous. Such a communication architecture does not care where the data comes from, but what the data is. The proxy network is responsible for matching event types and passing data to the appropriate subscribers. Automatically attached by event type, the consumer describes its needs by event type, even if the data owner does not want to send data to it. Multiple users can subscribe to the same type of data, ie the communication architecture has the characteristics of multicast. The publish/subscribe paradigm removes the dialog constraint, that is, the source and endpoint that do not require communication, and the service interaction relies on the notification agent to implement routing and matching of events.

However, when multiple smart grid services are distributed over the Internet, sensitive data exchanged by ubiquitous services is vulnerable to eavesdropping and attacks. Without a secure access control architecture, this data is vulnerable to unauthorized access. The security requirements of this article focus on access control and data confidentiality, that is, data publishers do not want unauthorized subscribers to access their published data. Each service message is independent of its publisher and subscriber, and multiple rounds of communication messages form a session. Smart grid services interact in the form of sessions and their interactions are data-centric. Based on the characteristics of publish/subscribe service and data-centric service interaction, this paper proposes a data-centric security mechanism to achieve the goal of access control and data confidentiality protection. Due to the indirect, anonymous and multicast interactions between publishers and subscribers, the existing access control mechanisms are not suitable for large-scale smart grid services. If more users are involved, symmetric key is not suitable for large-scale smart grid applications. In addition, the privacy of the publisher is not protected, and the subscriber knows who has subscribed to the data it publishes. The data in smart grid need to be integrated in the network before reaching the end users. For example, the intermediate agent can add the readings of smart meters owned by the same publisher to improve the effectiveness of data interaction. The requirement of intra network integration increases the difficulty of designing access control for smart grid services. At present, there is no relevant mechanism that can support access control and Intranet integration at the same time, such as attribute based encryption mechanism and authentication mechanism. Users design extensible access control mechanism in publish / subscribe system. However, these encryption mechanisms are not homomorphic and cannot be supported. The intranet integrates encrypted data. This paper proposes a data centric access control architecture (DCACF), as shown in Figure 2, which supports access control in smart grid services and data integration in the network. In this architecture, the publisher uses the private key based on homomorphic encryption mechanism to encrypt the published data.

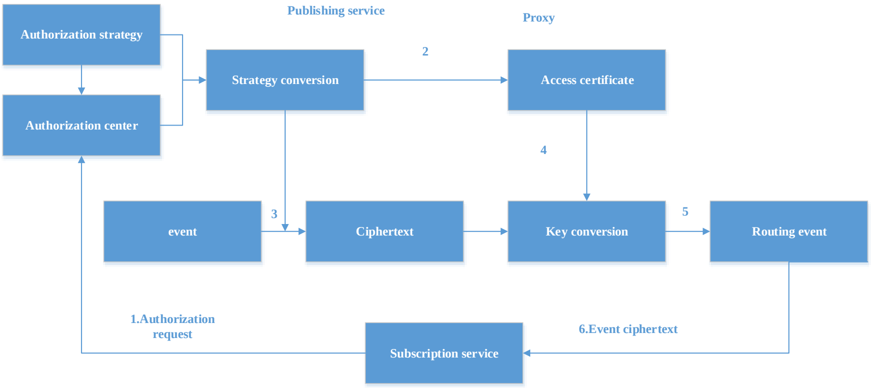

Figure 2. DCACF architecture

Prior to encryption, the data is bound with a random number representing the type of event, so that the encrypted data can only be decrypted by subscribers of this type of data with access rights. The intranet integration mentioned here is the integrated data itself, not a random number representing the event type attached to the same cryptograph. If the random number changes, the cryptograph becomes a unintelligible entity, which eventually leads to decryption failure. To maintain the homomorphic character, the DCACF architecture ensures that homomorphic operations affect only the data and do not change the random number representing the event type in the same cryptograph.In the proposed architecture, each potential subscriber gets an encryption event of a special event type and an access certificate. After the publisher receives the access request for the event type, it will generate the subscriber's access credentials based on the event type's access control policy and distribute those certificates to all Tanzhi agents. Access control policies are encoded as bloon filters and are included in the access certificate. When the intermediate agent receives an encryption event, it uses the bloon filter and the properties of the registered subscriber to check that the subscriber is qualified. For qualified subscribers, the intermediate agent uses the subscriber's public key to re encrypt the event, and the subscriber decrypts the encrypted event with its private key. Unlike the access control mechanism in DOS security standard, the publisher and subscriber do not need to share the key, which reduces the burden of key management of intermediate agent.

III. Experiments

This experiment uses a fully homomorphic encryption mechanism, which can effectively encrypt large integers. If the public mode g =100000000000031 is selected as the parameter, the plaintext in Z9 can be as large as 10M. We extended Apache ActiveMQ, a JMS middleware. The extension method is to construct a homomorphic operation on the publisher, build a key translation on a secure intermediate proxy, and build a homomorphic decryption on the subscriber. In the first step, the publisher encrypts the events that need to be published, the intermediate agent provides a release filter that publishes the event, and the key converts the encrypted event. The intermediate agent provides the subscriber's filter, which is the authorization policy of the subscription service. The subscriber decrypts the ciphertext converted by the conversion key. This experiment was conducted in a distributed test environment. Since it is difficult to estimate the performance in the publish/subscribe system without the same synchronous clock, the subscriber and the publisher are run on the same server. The server is configured as 8.0G RAM, Intel Windows 7, 64 operating system. The intermediate agent runs on other servers. The server configuration is 4.0G RAM, Intel Windows 7 operating system. The Publisher/Subscriber and Intermediate The agent is connected via a standard 100Mbps local area network. In the implementation, delay is the main performance indicator.There are two kinds of delays: one is to not join the access control mechanism, the total time from the publisher sending the event to the time the subscriber receives the event, including the matching time of the intermediate agent; The other is to join the access control mechanism, from the time the publisher encrypts the published event to the time the subscriber needs to decrypt the subscribed event. The latter mainly consists of three parts of delay: (1) the time of the publisher's encryption event, and (2) the time of the intermediate agent's key conversion, that is, the intermediate agent receives the encrypted event, and sends the converted re-encryption event. Time, (3) the time at which the recipient decrypts the re-encryption event. Through testing, we evaluated two aspects: one is the impact of the size of the publisher's published packet on performance, and the other is the performance impact of the number of attribute connections in the authorization policy.

IV. Discussion

To ensure the accuracy of the test results, each test case was run 1000 times. Figure 3 shows when you are not joining the access control architecture (Pub-to-Sub With Plain) and join the access control architecture (Pub-to-Sub with When the ACF), to publish data from the policy average delay (in number of the received data in different rules: ms), the size of the data is fixed (256 Bytes) . The horizontal coordinate indicates the size of the rule in the linear range of I, that is, 2 , 4 , 6 , 8 , 10, and the vertical coordinate indicates the delay. As show Figure 3, the number of rules increases, Pub -to-sub With The delay of ACF is slowly increasing.

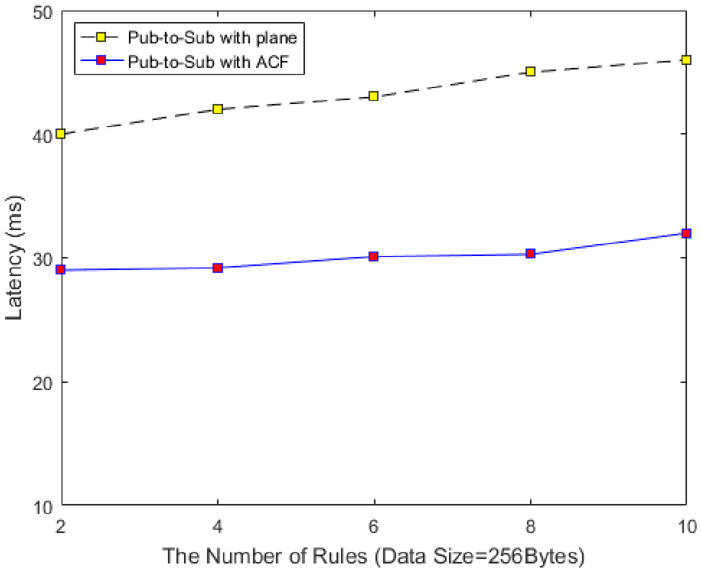

Figure 3. The number of data blocks affects the delay

This shows that the access control architecture devised in this paper has a good scalability in the number of attribute connections in the policy. An event, different packet sizes (from 1KB to 5KB), estimated performance shown in Figure 4. With the size distribution data variation can be observed in the original publish / subscribe system and added to the access control architecture overall delay (ACF) publish / subscribe system, the delay changes linearly, and it changes slowly. This means that the access control architecture devised in this paper can support arbitrarily large data. In all testing, CPU utilization, between 15% and 50%.

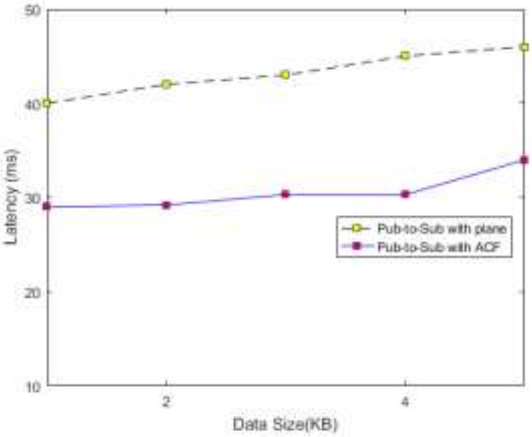

Figure 4. Effect of packet size on delay

As can be seen from the above delay estimation results,the proposed DCA CF architecture expanded the size of the size of the encrypted data, encryption can support large data.The publish/subscribe model is suitable for building a communication architecture for collaborative smart grid services. In publish/subscribe services, Qi part proposes a data-centric smart grid access control architecture, which maintains the anonymity, multicast and indirect communication characteristics of the publish/subscribe model. In this architecture, publishers and subscribers do not need to share keys, so there is no burden of key management. In addition, the architecture is based on homomorphic encryption, which supports in-network integration of encrypted data.This paper also analyzes the correctness and security of the proposed architecture. Preliminary estimates indicate that the implementation of the security section of this article proposed based publish/subscribe access control architecture has a good performance, and provides strong security capabilities (authorization and data confidentiality).

V. Conclusions

With the increasing openness and wide application of IoT systems, the privacy protection and security issues in the collaborative interaction of IoT services are facing new challenges. This paper proposes a secure data sharing mechanism for the data sharing, service collaboration, composition and user privacy aspects of the IoT environment. The I/O service interaction access control mechanism based on the publish/subscribe system protects the data. Privacy and access control for implementing services. Aiming at the communication between large-scale collaborative services, this paper builds an access control architecture suitable for large-scale distributed IoT service collaborative communication facilities and management service collaborative interaction based on the publish/subscribe paradigm, which realizes the confidentiality of data exchange between services. Privacy protection of service policies. Based on the communication facilities, this paper has done two aspects. On the one hand, it proposes a data-centric access control architecture (DCACF) to implement access control for service sessions and protect the confidentiality of interactive data. The main idea of DCACF is to attach an access control policy to the event, making the event an independent, meaningful entity. This architecture not only supports scalable smart grid service interactions, but also maintains service indirect, anonymous, multicast interaction features and data confidentiality. The use of fully homomorphic encryption technology to achieve intra-grid integration of encrypted data. The control strategy and access credentials of the encrypted data satellite code enable the collaborative service to perform indirect access control. The other party) proposes a two-layer access control architecture, while achieving the confidentiality of the data layer publishing events and the application layer protection of the service policy privacy. The main idea of the architecture is to propose two-way matching attributes and privacy policy requirements for the two-tier access control architecture, embedding policy embedding, policy and attribute blinding and encoding using anonymous sets.

Acknowledgement

The paper was supported by the engineering technology research center of web application software in Zhengzhou, 2021 Henan Province Key R&D and Promotion Special (Technology Tackling Key) Project (212102310572): Research on Key Technologies of Intelligent Educational System Based on Big Data Application.

References

[1] Islam N, Islam N. Botnets and Internet of Things Security. Computer, 2017, 50(2):76-79.

[2] Fernandes E, Rahmati A, Eykholt K, et al. Internet of Things Security Research: A Rehash of Old Ideas or New Intellectual Challenges?. IEEE Security & Privacy, 2017, 15(4):79-84.

[3] Maple C. Security and privacy in the internet of things. Journal of Cyber Policy, 2017, 2(2):155-184.

[4] Anitha A. Home security system using internet of things. IOP Conference Series: Materials Science and Engineering, 2017, 263:042026.

[5] Kolias C, Meng W, Kambourakis G, et al. Security, Privacy, and Trust on Internet of Things. Wireless Communications and Mobile Computing, 2019, 2019:1-3.

[6] Younis M, Akkaya K, Youssef M. Handling QoS Traffic in Wireless Sensor Networks. IEEE Journal on Selected Areas in Communications, 2015, 28(7):1105-1115.

[7] Illiano V P, Lupu E C. Detecting Malicious Data Injections in Wireless Sensor Networks: A Survey. Acm Computing Surveys, 2015, 48(2):1-33.

[8] Kapileswar N, Hancke G P. A Survey on Urban Traffic Management System Using Wireless Sensor Networks:. Sensors, 2016, 16(2):157.

[9] Ndiaye M, Hancke G P, Abu-Mahfouz A M. Software Defined Networking for Improved Wireless Sensor Network Management: A Survey. Sensors, 2017, 17(5):1031.

[10] Chen Z, Liu A, Li Z, et al. Distributed duty cycle control for delay improvement in wireless sensor networks. Peer-to-Peer Networking and Applications, 2016, 10(3):1-20.

[11] Malaver A, Motta N, Corke P, et al. Development and Integration of a Solar Powered Unmanned Aerial Vehicle and a Wireless Sensor Network to Monitor Greenhouse Gases. Sensors, 2015, 15(2):4072-4096.

[12] Khan I, Belqasmi F, Glitho R, et al. Wireless sensor network virtualization: A survey. IEEE Communications Surveys & Tutorials, 2017, 18(1):553-576.

[13] Rashid B, Rehmani M H. Applications of wireless sensor networks for urban areas: A survey. Journal of Network & Computer Applications, 2016, 60:192-219.

[14] Liu X Y, Zhu Y, Kong L, et al. CDC: Compressive Data Collection for Wireless Sensor Networks. IEEE Transactions on Parallel & Distributed Systems, 2015, 26(8):2188-2197.

[15] Zhang Y, Liu W, Lou W, et al. Location-based compromise tolerant security mechanisms in wireless sensor networks. IEEE Journal on Selected Areas in Communications, 2015, 24(2):247-260.

[16] Srbinovska M, Gavrovski C, Dimcev V, et al. Environmental parameters monitoring in precision agriculture using wireless sensor networks. Journal of Cleaner Production, 2015, 88:297-307.

[17] Fadel E, Gungor V C, Nassef L, et al. A survey on wireless sensor networks for smart grid. Computer Communications, 2015, 71(C):22-33.

[18] Khan I, Belqasmi F, Glitho R, et al. Wireless sensor network virtualization: early architecture and research perspectives. Network IEEE, 2016, 29(3):104-112.

[19] Xia S, Zou J, Zhu X, et al. Improvement on DV-Hop localization algorithm in wireless sensor networks. Journal of Computer Applications, 2015, 46(11):112-114.

[20] Rezvani M, Ignjatovic A, Bertino E, et al. Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Collusion Attacks. Dependable & Secure Computing IEEE Transactions on, 2015, 12(1):98-110.

[21] Rong P, Manli Z, Chi G, et al. Public Bicycle Operating System Based on Space-Time Security and the Internet of Things. Wuhan University Journal of Natural Sciences, 2018, 23(6):541-548.

[22] Wu, Fan, Xu, et al. A privacy-preserving and provable user authentication scheme for wireless sensor networks based on Internet of Things security. Journal of Ambient Intelligence & Humanized Computing, 2017, 8(1):101-116.

[23] Villari M, Fazio M, Dustdar S, et al. Software Defined Membrane: Policy-Driven Edge and Internet of Things Security. IEEE Cloud Computing, 2017, 4(4):92-99.